REMARKS

To date, the Examiner has not indicated that the subject matter of the information disclosure statement (IDS) filed January 17, 2006 has been properly considered. A copy of such IDS is submitted herewith. If the Examiner requires additional copies of any reference(s), applicant invites the Examiner to contact the undersigned. Documentation in the file wrapper of the instant application confirming the Examiner's consideration of the appropriate reference(s) is respectfully requested.

The Examiner has rejected Claims 1-7, 13-19, and 22-23 under 35 U.S.C. 103(a) as being unpatentable over Tarquini (U.S. Publication No. 2003/0101353) in view of Smith et al. ("Know Your Enemy: Passive Fingerprinting"). Further, the Examiner has rejected Claims 8-12, 20, 21, and 24-26 under 35 U.S.C. 103(a) as being unpatentable over Tarquini in view of Smith et al. further in view of Park (U.S. Patent No. 6,725,046). Applicant respectfully disagrees with such rejections, especially in view of the amendments made hereinabove to each of the independent claims.

Applicant respectfully points out that the Smith et al. reference ("Know Your Enemy: Passive Fingerprinting") has a last modified date of March 4, 2002. Applicant filed a priority document for the above application on January 15, 2002. As a result, the Smith et al. reference postdates applicant's priority date, and is therefore an improper reference. Thus, a notice of allowance or proper prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Despite the foregoing deficiency and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims to further distinguish applicant's claim language from the above reference(s), as follows:

> "wherein the data packets each include RFC-compliant TCP packets" (see this or similar, but not necessarily identical language in each of the independent claims).

Applicant respectfully points out that this amendment language is found in the following paragraph from applicant's specification:

> "The use of RFC-compliant TCP packets advantageously reduces the probability that the detection packets are blocked by a router or firewall, and greatly reduces the probability that the detection packets will cause damage or crashes at the target computer." (Paragraph 80)

The Tarquini reference teaches sending "a series of carefully designed TCP packets, or probes, to one or more hosts of the targeted system"(page 7, [0043]) (emphasis added). In contrast, applicant claims the transmission of data packets that "each include RFC-compliant TCP packets"(emphasis added). The Tarquini reference makes no reference to the use of RFC-compliant TCP packets, and, as a result, applicant's claims are distinct from the prior art. Further, as noted in the above excerpt from applicant's specification, such compliancy may optionally, in some embodiments, advantageously reduce the probability that detection packets are blocked by a router or firewall, and reduce the probability that the detection packets will cause damage or crashes at a target computer.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claim 7, the Examiner has relied on the following excerpts from the above reference to make a prior art showing of applicant's claimed system "wherein said protocol is TCP/IP and wherein said first range of bits corresponds to a packet field representing a maximum segment size."

> "Each operating system of a node incorporating an instance of an IPS application additionally comprises a network protocol stack 90, as illustrated in FIG. 3, that defines the entry point for frames received by a targeted node from the network, e.g. the Internet or Intranet. Network stack 90 as illustrated is representative of the well-known WindowsNT (TM) system network protocol stack and is so chosen to facilitate discussion and understanding of the invention. However, it should be understood that the invention is not limited to a specific implementation of the illustrated network stack 90 but, rather, stack 90 is described to facilitate understanding of the invention. Network stack 90 comprises a transport driver interface (TDI) 125, a

> transport driver 130, a protocol driver 135 and a media access control (MAC) driver 145 that interfaces with the physical media 101. Transport driver interface 125 functions to interface the transport driver 130 with higher-level file system drivers. Accordingly, TDI 125 enables operating system drivers, such as network redirectors, to activate a session, or bind, with the appropriate protocol driver 135. Accordingly, a redirector can access the appropriate protocol, for example UDP, TCP, NetBEUI or other network or transport layer protocol, thereby making the redirector protocol-independent. The protocol driver 135 creates data packets that are sent from the computer hosting the network protocol stack 90 to another computer or device on the network or another network via the physical media 101. Typical protocols supported by an NT network protocol stack comprise NetBEUI, TCP/IP, NWLink, Data Link Control (DLC) and AppleTalk although other transport and/or network protocols may be comprised. MAC driver 145, for example an Ethernet driver, a token ring driver or other networking driver, provides appropriate formatting and interfacing with the physical media 101 such as a coaxial cable or another transmission medium." (page 5, [0032])

After careful review of the foregoing excerpt, it is clear that no mention is made in the above Tarquini excerpt regarding applicant's claimed technique "wherein said first range of bits corresponds to a packet field representing a maximum segment size" (emphasis added). Since the above excerpt fails to mention both a range of bits corresponding to a packet field as well as a packet field representing a maximum packet size, applicant's claim is distinct from the Tarquini reference.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 52-56 below, which are added for full consideration:

> "wherein the third data packet includes an RFC-compliant TCP packet" (see Claim 52);
>
> "wherein the first data packet includes a TCP SYN packet with a maximum segment size MSS option in an options field thereof set to 0" (see Claim 53);
>
> "wherein the first data packet includes a TCP SYN packet with a maximum segment size MSS option in an options field thereof set to 128" (see Claim 54);
>
> "wherein at least one of the fingerprints includes the following format:
> $AW_{MSS=0}$:$AW_{MSS=128}$:$AW_{MSS=384}$:TTL:DF:OS,
>
> where:
> AW refers to a TCP advertised window,
> MSS refers to a TCP options maximum segment size,
> TTL refers to a TCP options time to live,
> DF refers to a TCP options don't fragment flag, and
> OS refers to an operating system identification" (see Claim 55); and
>
> "wherein at least one of the target computer fingerprints includes the following format:

$AW_{MSS=0}$:$AW_{MSS=128}$:$AW_{MSS=384}$:$OPT_{MSS=384}$:$OPT_{MSS=0}$:$OPT_{MSS=128}$:TTL:DF:FL:OS,

where:

OPT refers to TCP options bytes, and

FL refers to TCP flags" (see Claim 56).

Again, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P327/02.240.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	
Stuart C. McClure et al.	Group Art Unit: 2157
Application No. 10/050,675	Examiner: Sall, E.
Filed: January 15, 2002	Date: January 12, 2006
For: SYSTEM AND METHOD FOR NETWORK VULNERABILITY DETECTION AND REPORTING	

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450 on the date listed above.

Signed: Erica L. Farlow

Erica L. Farlow

INFORMATION DISCLOSURE STATEMENT
UNDER 37 CFR §§1.56 AND 1.97(c)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

The reference(s) listed in the attached PTO Form 1449, cop(ies) of which is attached (when necessary), may be material to examination of the above-identified patent application. Applicants submit the reference(s) in compliance with their duty of disclosure pursuant to 37 CFR §§ 1.56 and 1.97. The Examiner is requested to make the reference(s) of official record in this application.

This Information Disclosure Statement is not to be construed as a representation that a search has been made, that additional information material to the examination of this application does not exist, or that the reference(s) indeed constitutes prior art.

This Information Disclosure Statement is being filed after the mailing date of a first Office Action. Accordingly, applicants are including a payment in the amount of $180.00 for the fee due in connection with the filing of this Information Disclosure Statement. However, if it is determined that any additional fees are due, the Commissioner is hereby authorized to charge such fees or credit any overpayment to Deposit Account 50-1351 (Order No. NAI1P327).

Respectfully submitted,
Zilka-Kotab, PC

Kevin J. Zilka
Reg. No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
Telephone: (408) 971-2573

Form 1449 (Modified) **Information Disclosure Statement By Applicant** (Use Several Sheets if Necessary)	Atty. Docket No. NAI1P327/02.240.01 Applicant: S. McClure et al. Filing Date: 01/15/2002	Application No.: 10/050,675 Group Art Unit: 2157

U.S. Patent Documents

Examiner Initial	No.	Patent No.	Date	Patentee	Class	Sub-class	Filing Date
	A	6,266,774	07/24/2001	Sampath et al.	713	201	12/08/1998
	B	6,282,546	08/28/2001	Gleichauf et al.	707	102	06/30/1998
	C	6,301,668	10/09/2001	Gleichauf et al.	713	201	12/29/1998
	D	6,324,656	11/27/2001	Gleichauf et al.	714	37	06/30/1998
	E	2001/0034847	10/25/2001	Gaul, Jr.	713	201	03/27/2001
	F						
	G						
	H						
	I						
	J						
	K						

Foreign Patent or Published Foreign Patent Application

Examiner Initial	No.	Document No.	Publication Date	Country or Patent Office	Class	Sub-class	Translation	
							Yes	No
	L							
	M							
	N							
	O							
	P							

Other Documents

Examiner Initial	No.	Author, Title, Date, Place (e.g. Journal) of Publication
	R	
	S	
	T	

Examiner	Date Considered

Examiner: Initial citation considered. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

COPY

PATENT POSTCARD

Docket No. NAI1P327/02.240.01 Appln. No.: 10/050,675 Date: 01/12/2006

By: KJZ:ELF Filing Date: 01/15/2002 Express Mail No.:

Inventor(s): Stuart C. McClure et al.

Title: SYSTEM AND METHOD FOR NETWORK VULNERABILITY DETECTION AND REPORTING

The following has been received in the U.S. Patent & Trademark Office on the date stamped below:

X Information Disclosure Statement
X PTO Form 1449
X Check in the amount of $180.00
X Return Receipt Postcard

1/30/06